UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	**3:CR-20-197**
v.	**:**	**(JUDGE MANNION)**
THOMAS J. HART,	**:**	
Defendant	**:**	

M E M O R A N D U M

Presently before the court is the Motion to Suppress Seizure of Electronic Communications, (Doc. 32), filed by defendant Thomas J. Hart through his counsel. Specifically, Hart, who was charged with one count of knowingly receiving and distributing child pornography, in violation of 18 U.S.C. §2252(a)(2), moved to suppress electronic communications that he allegedly sent on a Kik messenger app containing child pornography files and videos, after Kik provided them through a CyberTipline Report ("Cybertip") to the National Center for Missing and Exploited Children ("NCMEC"). The Cybertip was eventually sent to the FBI. Hart also seeks to suppress the evidence seized by the FBI from Kik's Cybertip based on a discrepancy between the number of videos the FBI identified and the actual number of video files that were included with the Cybertip. Thus, Hart claims that the FBI's search exceeded the scope of the search performed by Kik. The pending motion has been fully briefed, Exhibits were submitted, and the motion is now ripe

for disposition. Based on the following, defendant Hart's motion to suppress will be **DENIED IN ITS ENTIRETY** without the necessity of conducting an evidentiary hearing.

I. FACTUAL AND PROCEDURAL HISTORY

Kik is a freeware instant messaging mobile application ("app"), and is a "provider" pursuant to 18 U.S.C. §§2258E and 2510. On February 19, 2020, Kik submitted a Cybertip, regarding the distribution of videos apparently depicting child pornography, to NCMEC pertaining to one of its users by the name of "televiper", who was later identified as Hart. The Cybertip indicates that Kik viewed the "entire contents of the files." The total number of files that Kik uploaded to NCMEC in its Cybertip was 12 files. Specifically, the Cybertip contained 11 video files and one .pdf file. (*See* D's Ex. 1, Doc. 33-1). Kik's Cybertip indicated that 11 child pornography videos, including some duplicates, were distributed via Kik using private chat messages and group messaging. See, Def. Ex. 1. The twelfth file uploaded by K[ik] for its Cybertip to NCMEC had the filename "Subscriber-data-televiper_2th. .pdf", which consisted of a [.pdf] file containing account information about the K[ik] user. (*See* D's Ex. 1, Doc. 33-1 at 6 and 11).

On March 27, 2020, NCMEC forwarded the Cybertip it received from Kik to the Pennsylvania Internet Crimes Against Children ("ICAC") Task Force, in Media,

Delaware County, Pennsylvania. The images included with the Cybertip were not reviewed by NCMEC before it sent the Cybertip to ICAC. (D Ex. 1, Doc. 33-1 at 11). After receiving the Cybertip, ICAC forwarded it to the Federal Bureau of Investigation ("FBI") Philadelphia Office, and eventually it was sent to the FBI Scranton, PA, Resident Office.

The Cybertip, which contained the 11 video files and 1 .pdf file, was assigned to FBI Special Agent Eric Bailey for investigation. Agent Bailey determined that there were eight total unique video files containing child pornography. Some images depicting child pornography were uploaded multiple times, and in total there were 11 uploads.

The FBI then conducted an investigation and discovered that Hart, who lived in Pittston, Luzerne County, Pennsylvania, created the Kik account with the username "televiper." On August 12, 2020, the FBI, along with other agencies, executed a search warrant approved by a Magistrate Judge at Hart's house in Pittston. The search of Hart's house, including devices in the house, did not reveal any images of sexual exploitation of minors. Hart was also interviewed and he admitted to using the Kik mobile app in his cell phone to participate in group chats with others. In particular, Hart admitted to using the "televiper" account on the Kik app to participate in chat groups where child pornography was shared between the individuals in the groups. Hart admitted that he would take the child pornography

pictures and videos from one chat group and post them into other chat groups to which he belonged.

Later on August 12, 2020, Agent Bailey filed a criminal complaint against Hart charging him with one count of distribution of child pornography, in violation of 18 U.S.C. §2252(a)(2). (Doc. 1). A Magistrate Judge conducted an initial appearance, (Doc. 7), and subsequently, on August 14, 2020, Hart was released on bail. (Doc. 9). On August 25, 2020, Hart was indicted by a Grand Jury on one count of distribution of child pornography, in violation of §2252(a)(2). (Doc. 13). On August 28, 2020, Hart was arraigned and he was continued on pretrial release. (Doc. 17).

On April 12, 2021, Hart filed his motion to suppress the seizure of electronic communications and his brief in support, with a 12-page Exhibit, namely, the Cybertip Report. (Docs. 32, 33 & 33-1).

After being granted an extension of time, the government filed its brief in opposition on May 17, 2021. Hart did not file a reply brief and the time within which to do so has expired.

The trial which had been scheduled in this case to commence on June 7, 2021, was continued generally until the court ruled on Hart's suppression motion.

II. LEGAL STANDARD

The court has jurisdiction over Hart's motion to suppress under 18 U.S.C. §3231. A criminal defendant brings a pre-trial motion to suppress evidence under Federal Rule of Criminal Procedure 12(b)(3)(C), in an effort "to show that evidence against him or her was unconstitutionally obtained." U.S. v. Hernandez, 2015 WL 5123924, at *4 (M.D. Pa. 2015). Protection against unreasonable searches and seizures is enshrined in the Fourth Amendment, which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
>
> U.S. Const. amend. IV.

"The Fourth Amendment, like the other Amendments contained in the Bill of Rights, imposes direct limitations on the actions that may be taken by the Federal Government." Adams v. Springmeyer, 17 F.Supp.3d 478, 490 (W.D. Pa. 2014) (citing McDonald v. City of Chicago, 561 U.S. 742, 753–55 (2010)). The Fourth Amendment's purpose is to "safeguard the privacy and security of individuals against arbitrary invasions" by the government. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967). For purposes of the Fourth Amendment, a search "occurs when an expectation of privacy that society is prepared to consider as reasonable

is infringed." United States v. Jacobsen, 466 U.S. 109, 113 (1984). In order to establish standing under the Fourth Amendment to challenge a search, a defendant must show a "reasonable expectation of privacy" in the place or thing searched. Rakas v. Illinois, 439 U.S. 128, 132 n.1 (1978).

If standing is established, then the court examines the search warrant or lack thereof. The burden of persuasion depends on whether or not there was a warrant that authorized the search. *See* Hernandez, 2015 WL 5123924, at *4. Further, the Supreme Court regards exclusion of evidence as an "extreme sanction" that "should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule," which center on deterring police misconduct. U.S. v. Leon, 468 U.S. 916, 918 (1984).

The Fourth Amendment also lays out four requirements of a valid search warrant. The warrant must: 1) be based on probable cause; 2) be supported by a sworn affidavit; 3) describe particularly the place of the search; and 4) describe particularly the persons or things to be seized. Groh v. Ramirez, 540 U.S. 551, 557 (2004).

"The Fourth Amendment requires that a search warrant be supported by probable cause, and '[e]vidence seized pursuant to a search warrant that is not so supported may be suppressed.'" U.S. v. Rivera, 524 Fed.Appx. 821, 825 (3d Cir. 2013) (citation omitted).

The district court conducts only a deferential review of the initial probable cause determination made by the magistrate [judge] regarding a search. U.S v. Stearns, 597 F.3d 540, 554 (3d Cir. 2010) (citing Illinois v. Gates, 462 U.S. 213, 236, 103 S.Ct. 2317 (1983)). "The role of a reviewing court is not to decide probable cause *de novo*, but to determine whether 'the magistrate [judge] had a substantial basis for concluding that probable cause existed.'" *Id*. (citation omitted). In order for the reviewing court to make this determination, it "must consider the totality of the circumstances, 'and need not conclude that it was more likely than not' that the evidence sought was at the place described." Rivera, 524 Fed.Appx. at 825 (citation omitted). "If a substantial basis exists to support the magistrate [judge]'s probable cause finding, [the court] must uphold that finding ...." Stearns, 597 F.3d at 554. In evaluating a search warrant application, "the magistrate [judge] must 'make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *Id*. (citation omitted). A search warrant can be issued even when supported by an affidavit which does not contain direct evidence linking the crime with the place to be searched. Id. "Probable cause can be, and often is, inferred from 'the type of crime, the nature of the items sought, the suspect's opportunity for concealment and normal inferences about where a criminal might hide [evidence].'" *Id.* (citation omitted). "[T]he resolution of doubtful

or marginal cases in this area should be largely determined by the preference to be accorded to warrants." U.S. v. Jones, 994 F.2d 1051, 1055 (3d Cir. 1993) (citation omitted).

The court's "role is not to make [its] own assessment as to whether probable cause existed", "[r]ather, [it is] constrained to determine only whether the affidavit provides a sufficient basis for the decision the magistrate judge actually made." Jones, 994 F.2d at 1057. Thus, the district court's limited role is to determine if the four corners of the affidavit in support of the search warrant provided "the magistrate judge with a substantial basis on which to conclude that evidence of a crime would be found in the defendant['s] residence[]." *Id*. at 1055.

"Under the exclusionary rule 'evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure.'" Lara-Mejia, 482 F.Supp.3d at 293 (quoting United States v. Calandra, 414 U.S. 338, 347, 94 S.Ct. 613, 38 L.Ed.2d 561, (1974)). "This prohibition also applies 'to the fruits of the illegally seized evidence.'" *Id*. "The rule operates as 'a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.'" *Id*. (citations omitted).

Generally, "the burden of proof is on the defendant who seeks to suppress evidence." U.S. v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995) (citation omitted).

"However, once the defendant has established a basis for his motion, [], the burden shifts to the government to show that the search or seizure was reasonable." *Id*. (citation omitted).

III. DISCUSSION

As mentioned *supra*, Hart has filed a pre-trial motion to suppress evidence consisting of the electronic files with child pornography content found under his "televiper" username that were contained in the Cybertip Kik sent to NCMEC arguing that Kik's monitoring of the users' files on its app constituted governmental action that was an unlawful search without a warrant in violation the 4th Amendment. Hart argues that the warrantless seizure and search of his electronic communications constituted governmental action by Kik since the statute, 18 U.S.C.A. §2258A(b), "coerced" Kik to report apparent child pornography via a Cybertip. As such, Hart contends that since he had a reasonable expectation of privacy in the communications that he made on the Kik app, "[w]hen the government coerced K[ik] into using a government backed reporting mechanism, K[ik] becomes a government actor", and that "K[ik] violated [his] Fourth Amendment rights to be free from unreasonable searches and seizures by seizing the images and passing them along to NCMEC." (Doc. 33 at 5-6).

The government contends that Kik is not a governmental agency and that its conduct was a private search that did not implicate the 4th Amendment.

No doubt that "[t]he Fourth Amendment regulates state actors", and "private parties are only bound by its requirements insofar as they operate as *de facto* state actors." U.S. v. DiTomasso, 81 F.Supp.3d 304, 306 (S.D. N.Y. 2015), *aff'd*, 932 F.3d 58 (2d Cir. 2019), *cert. denied*, 141 S.Ct. 314 (2020). Further, the Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official." *Id*. (citation omitted).

> One way for a private party to "act[ ] as an agent of the Government" is through legal compulsion. If a private party must perform a search—if she can face liability for not doing so—the search "is controlled by the Fourth Amendment." But legal compulsion is not necessary for an otherwise-private search to be subject to the Fourth Amendment's requirements. A search carried out voluntarily by a private actor will still be subject to the Fourth Amendment's strictures if the government "demonstrate[s] a strong [ ] preference for [the search]."

Id. at 308 (citations omitted).

A private party can also act as a government agent if its performs "searches with an intent to assist law enforcement." *Id*. at 309 (citation omitted). However, "private actions are generally attributable to the government only where there is a sufficiently close nexus between the State and the challenged action of the ... entity so that the action of the latter may be fairly treated as that of the State itself."

DiTomasso, 93 F.3d at 67-68 (internal quotations marks and citations omitted). "The requisite nexus is not shown merely by government approval of or acquiescence in the activity, or by the fact that the entity is subject to government regulation." *Id*. at 68. "The purpose of the [close-nexus requirement] is to assure that constitutional standards are invoked only when it can be said that the [government] is responsible for the specific conduct of which the [accused] complains." *Id*. (internal quotations marks and citations omitted). *See also* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614, 109 S.Ct. 1402 (1989) ("Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities ....").

Here the court must determine whether Kik conducted the search at issue as an agent or instrument of the government or whether Kik's monitoring was "a purely private search beyond the reach of the Fourth Amendment." DiTomasso, 93 F.3d at 68.

The Third Circuit has not yet decided the contours of the law regarding whether private party electronic communication providers and messaging services, such as Kik, act as agents of the government "when they monitor their users' activities on their servers, or when they implement their own internal security

measures against users engaging in illegal activity through their serv[ers]", (Doc. 37 at 7), and whether their activities must conform to the 4th Amendment.

The test utilized in the Sixth Circuit is "that a private actor's reason for performing a search must be 'entirely independent of the government's intent to collect evidence for use in a criminal prosecution' to escape Fourth Amendment scrutiny." DiTomasso, 81 F.Supp.3d at 309 (citation omitted). In the Ninth Circuit, the Court "has held that an otherwise-private search must comply with the Fourth Amendment if 'its purpose [is] to elicit a benefit for the government in either its investigative or administrative capacities.'" *Id*. (citation omitted). In DiTomasso, *id*. n. 33, the district court found that "law enforcement purpose was one factor to consider when analyzing whether a search is purely private", and noted that "'the private party's intent in executing the search' has been deemed relevant to the Fourth Amendment analysis by the First, Sixth, Ninth, and Tenth Circuits."

The court now considers this issue and finds that Kik was not acting as a government agency and that it was not acting as an agent of law enforcement when it submitted the Cybertip at issue, regarding files which appeared to contain evidence of child pornography, to NCMEC.

Kik, as a "provider" under 18 U.S.C. §§2258E and 2510, was obliged to send the Cybertip to NCMEC "under section 2258A of the PROJECT Our Children Act, [18 U.S.C. §2258A(a)(1)], which requires any private entity that 'obtains actual

knowledge' of child pornography trafficking to notify NCMEC." DiTomasso, 81 F.Supp.3d at 306. "NCMEC is a private, nonprofit corporation, which aims to reunite families with missing children, reduce child sexual exploitation, and prevent the victimization of children." DiTomasso, 932 F.3d at 61. Further, "[NCMEC] maintains an initiative whereby individual persons and ISPs can report to [it] on a range of internet-based misconduct, including the apparent presence of child pornography." *Id*. "Once child pornography conduct has been reported to NCMEC, NCMEC is required to 'forward' any such report to law enforcement." DiTomasso, 932 F.3d at 61 (citing §2258A(c)(1)).

Additionally, as the district court in DiTomasso, 81 F.Supp.3d at 306, explained:

> The statute also provides a safe harbor for compliance. Under section 2258B, any entity that issues a NCMEC Report pursuant to its obligations under section 2258A is immunized from all liability, civil or criminal, that might otherwise have resulted from the nonconsensual disclosure of a user's electronic information. [Fn. omitted] There is, however, no statutory obligation to *look for* child pornography trafficking. Rather, the obligations of section 2258A are triggered only when an internet service provider ("ISP") like [Kik] obtains "actual knowledge" of such trafficking.

When an ISP "obtains actual knowledge" of unlawful conduct involving child pornography, "[it is] required by §2258A [] to report that conduct to NCMEC, 18 U.S.C. §2258A(a), and they face substantial fines if they fail to do so." DiTomasso, 932 F.3d at 61 (citing §2258A(e)).

As the government points out, (Doc. 37 at 7-8), "courts that have addressed the question [presented in this case as to whether Kik's monitoring activities was performed as an agent of the government] uniformly answer it in the negative." (citing United States v. Stratton, 2017 WL 169041, at *4 (D. Kansas Jan. 17, 2017) (holding that Sony was not a government agent when it searched images stored on the defendant's PS3); United States v. Richardson, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails); United States v. Stevenson, 727 F.3d 826, 831 (8th Cir. 2013) ("AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes.... AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass 2013) (AOL is not a government agent); United States v. Ackerman, 2014 WL 2968164, at *5-6 (D. Kan. July 1, 2014) (AOL is not a state actor), rev'd on other grounds, 831 F.3d 1292 (10th Cir. 2016); United States v. Drivdahl, 2014 WL 896734, at *3-4 (D. Mont. Mar. 6, 2014) (Google is not a Government agent); United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (Yahoo!, Inc., did not act as an agent in searching

e-mails and sending reports to NCMEC); [DiTomasso, *supra*] (chat service provider Omegle held not to be a Government agent and its search of defendant's chat messages held to be a pure private search beyond the reach of the Fourth Amendment); United States v. Miller, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015) (holding that Google is a "private, for profit entity" that "complied with its statutory duty to report violations of child pornography laws" and did not become a state actor by doing so)).

Hart argues that Kik acted as a government agent in conducting a warrantless search of his messaging and uploaded files since the government "coerced" Kik "into using a government backed reporting mechanism" based on the statute, 18 U.S.C. §2258A, requiring providers like Kik to report possible child exploitation. However, as the government states, (Doc. 37 at 9), "Kik [did not] lose or forfeit its status as a private party simply by [] complying with its legal obligation to report suspected criminal activity to NCMEC." As mentioned above, the requisite "close nexus" between the government and the challenged action of Kik required for Kik's action to be treated as that of the government is not shown merely "by the fact that [Kik] is subject to government regulation." DiTomasso, 932 F.3d at 68 (citations omitted). *See also* U.S. v. Miller, 982 F.3d 412, 424 (6th Cir. 2020) (holding that "private action [such as Google's activity of operating a system to detect child pornography and its requirement to notify NCMEC when it becomes

aware of child pornography] does not become government action merely because the government authorizes or acquiesces in it", and holding that [e]ven extensive regulation of a private party will not turn its every action into government action.").

Additionally, as the government states:

> Kik not only complied with the mandates of §2258A, but also used its discretion, as a private entity and provided additional information over and above what is statutorily required. Def. Ex. 1 [Doc. 33-1]. In its [Cybertip] report, Kik voluntarily chose to include the images, the dates and times of the upload and the Internet Protocol address.

(Doc. 37 at 9) (citing 18 U.S.C. §2258A(b)(1)-(5)).[1]

Recently, the Sixth Circuit in Miller, *supra*, considered whether "Google conducted an 'unreasonable search' by scanning [defendant's] July 9 email [which had two attached files containing child pornography images] for hash-value [matching images in Google's child-pornography repository]." Google then sent a Cybertip to NCMEC and no Google employee viewed the files. Ultimately the IP address associated with the Gmail account lead officers to the defendant. The Sixth Circuit stated that defendant's claim that Google's hash-value matching was an unreasonable search that violated the 4th Amendment "faces an immediate (and

[1]Under the statute, when a provider, such as Kik, submits a Cybertip to NCMEC it can include additional information, at its discretion, such as the following: (1) Information about the involved individual; (2) Information regarding the transmission of the content relating to the report; (3) geographic information of the involved individual; (4) visual depictions of apparent child pornography; and (5) the complete communications containing any visual depiction of apparent child pornography. 18 U.S.C. §2258A(b)(1)-(5).

ultimately insurmountable) obstacle: Google is a private entity", and that "[l]ike other constitutional rights, …, the Fourth Amendment regulates only government action." *Id*. at 421 (internal citations omitted). The Court stated that since the defendant was seeking to suppress evidence, "[he] must prove that Google's actions were government actions under one of the[] tests [i.e., traditional agency test, function test, compulsion test, or a nexus test]." *Id*. at 423 (citations omitted). The Court then examined the defendant's 4th Amendment claim regarding Google's monitoring activities under each of the stated tests. *Id*. at 424-25.

To paraphrase, the Sixth Circuit essentially found that "the initiative" for Google's decision to scan its customers' files came from "the private party, not the government." *Id*. at 424. The Court explained its finding by stating, in part, that even though "Federal law requires 'electronic communication service providers' like Google to notify NCMEC when they become aware of child pornography", "this mandate compels providers only to *report* child pornography that they know of; it does not compel them to *search* for child pornography of which they are unaware." *Id*. (internal citations omitted). The Court further stated that "the Supreme Court's cases tell us to focus on 'the specific conduct of which [a party] complains'", and "[t]hat conduct is Google's hash-value matching, not its reporting." *Id*. (internal citations omitted). The Court also pointed out that "[m]any courts have found that a 'reporting requirement, standing alone, does not transform [a service provider]

into a government agent whenever it chooses to scan files sent on its network for child pornography.'" *Id*. (string citations omitted). The Court also compared Google's responsibility under 18 U.S.C. §2258A(a) to notify NCMEC "to many laws [that] require certain individuals, such as teachers or doctors, to report child abuse", and stated that "[i]n that context, too, courts have held that reporting mandates do not transform private parties into government actors for purposes of various constitutional provisions." *Id*. (citations omitted).

Finally, the Miller Court found that under the nexus test, where private action may be "attributed to the government if a sufficiently close nexus exists between a private party and government actors", there was no evidence to show that Google intended to act as a government agent. *Id*. Rather, the Court stated that "Google … sought to rid its virtual spaces of criminal activity for the same reason that shopkeepers have sought to rid their physical spaces of criminal activity: to protect their businesses." *Id*. Similar to the Miller case, Hart does not cite to any evidence that either Agent Bailey or any officer influenced Kik's decision to monitor the chat group.

The Sixth Circuit concluded that since "child pornography is tragically common", "it makes sense for [service] providers [such as Google and Kik] that must report it to create a generic form for their 'convenience,' whether or not they have agreed with government actors to conduct searches." *Id*. at 426 (internal

citations omitted). Thus, the Miller Court found that Google's activity of scanning files of its users for hash-value matches to protect against its users sharing images of child pornography did not implicate the Fourth Amendment."[2] *Id*.

Kik had a proprietary interest in its product and it was certainly entitled to protect the value of its messaging service by monitoring it and by preventing it from being used to share files containing child pornography. In short, this court concurs with the well-reasoned decision of the Sixth Circuit in Miller, as well as the other cited cases, and concurs with their rationale, and will deny Hart's motion to suppress Kik's Cybertip Report, (*see* Doc. 33-1), since the court finds that Kik's warrantless search of Hart's messaging and uploaded files constituted a private search for 4th Amendment purposes that did not require a warrant.

Next, the court considers whether Agent Bailey's search exceeded the scope of Kik's search and whether it amounted to an unreasonable search and seizure under a trespass theory. Hart argues that even if Kik is a private entity, Bailey conducted an "unreasonable search" when he later opened and viewed the files sent by Kik. Hart states that since "[t]he CyberTipline report states that K[ik] viewed

[2]Google created its "own proprietary hashing technology to tag confirmed child sexual abuse images", and it "assigns a 'hash value' to a known image of child pornography and then scans its services for files with the same value." Miller, 982 F.3d at 419. In the present case, the Cybertip indicates that the apparent child pornography was based on NCMEC's review of the Report or a "hash match" of one or more uploaded files.

the entire contents of the video", "agent Bailey's further review of the materials was an independent trespass and invasion of [his] privacy." He further states that "Agent Bailey did not have a search warrant to open the file provided to him by NCMEC", and that "[n]o independent judicial review of the CyberTipline report was taken." (Doc. 33 at 6).

Hart basically points out that "the Supreme Court recently clarified that such a 'search' also occurs when the government trespasses onto property to obtain information." Miller, 982 F.3d at 418 (citing United States v. Jones, 565 U.S. 400, 404–08, 132 S.Ct. 945 (2012)). Hart also essentially claims that Bailey's warrantless opening and examination of the files in the Cybertip qualifies as a search in a "trespass-to-chattels" sense. *Id*.

In particular, Hart, (Doc. 33 at 9), argues as follows:

> Here, agent Bailey violated Mr. Hart's common law trespass, chattel, and replevin rights. Agent Bailey needed to take and open the files to see if they contained child pornography. Nothing in the ChildTipline report offers any description of what is contained. The videos could have contained private videos that were not child pornography, and as agent Bailey in the sealed affidavit to the search warrant only identified 6 unique videos of child pornography, this may in fact have been the case for some of the 12 videos. Under a common law trespass, chattel or replevin theory, agent Bailey took the files without permission and opened them. He did so without probable cause, without a warrant and without Mr. Hart's consent. These actions were an unreasonable search and do not fall under the private party doctrine.

Thus, Hart contends that since Bailey did not identify the correct number of videos containing child pornography in his affidavit of probable cause regarding

the search warrant application for Hart's house, he opened more files than contained in the Cybertip without a warrant, without permission, without probable cause, and without consent.

Under the "private search doctrine", a search by the government may be found to be permissible after a private party is responsible for the initial intrusion of a person's expectation of privacy, for example by opening an object and examining its contents, and then, after finding something suspicious, submits the object to the government which repeats the same examination of the object. Under the doctrine, "[t]he Supreme Court has concluded that even a 'wrongful search ... conducted by a private party does not violate the Fourth Amendment.'" U.S. v. Tolbert, 326 F.Supp.3d 1211, 1219 (D. N.M. 2018) (quoting Walter v. United States, 447 U.S. 649, 656, 100 S.Ct. 2395 (1980)). Also, "such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." *Id*. (citation omitted). The court in Tolbert, *id*., then explained:

> In United States v. Jacobsen, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), FedEx employees opened a damaged package, found suspicious plastic bags of white powder inside, and passed the parcel to the government, along with a description of what they had found. Id. at 111, 104 S.Ct. 1652. An agent from the Drug Enforcement Agency ("DEA") then repeated the same investigation, opening the package and examining its contents. *Id*. Finally, he subjected the white powder to a chemical drug test to confirm it was cocaine. *Id*. at 111-12, 104 S.Ct. 1652. Considering all this, the Supreme Court held that no "search" implicating the Fourth Amendment had taken place because there was a "virtual certainty" that the government could have discovered "nothing else of significance" in the package nor learned anything beyond what it had "already ... been told" by a private party.

> *Id*. at 119, 104 S.Ct. 1652. "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id*. at 117, 104 S.Ct. 1652.

No doubt that "[t]he Supreme Court has long required the government to obtain a warrant to open sealed letters, the equivalent of modern emails." Miller, 982 F.3d at 418 (citations omitted). However, "well before [United States v. Jacobsen, 466 U.S. 109, 104 S. Ct. 1652 (1984)], the Court also allowed the government to rely on letters illegally taken and opened by private parties." *Id*. (citation omitted). In the present case, the Cybertip Kik submitted to NCMEC included 12 files Kik uploaded to NCMEC, consisting of 11 video files and one .pdf file. Kik indicated that the 11 child pornographic videos were distributed on the Kik app using private chat messages and group messaging. Agent Bailey reviewed the 11 video files and one .pdf file provided in the Cybertip. Agent Bailey's search warrant affidavit incorrectly indicated a total of 7 unique videos were included with Kik's Cybertip but there were actually 8 distinct videos files that Bailey determined contained child pornography. It was also determined that some videos were uploaded multiple times which accounted for the total of 11 uploads.

As in the Miller case in which the Court indicated that "Google arguably 'opened' the files and committed the 'trespass'", *id*., the court finds that since Kik had opened the files in the instant case and NCMEC did not view the files before it sent them to law enforcement officials, it was a private party search that did not

violate the 4th Amendment and Agent Bailey's examination of the files did not constitute a search under the traditional trespass test.

As the government, (Doc. 37 at 9-10), explains:

> Agent Bailey merely reviewed information provided by a prior private search. Agent Bailey reviewed the video files solely after Kik had already done so and forwarded them to NCMEC. Agent Bailey's review of the video files contained in the CyberTipline Report did not constitute a "search" subject to Fourth Amendment scrutiny.

The Sixth Circuit in Miller, *id*. at 417-18, addressed a similar contention as raised by Hart, and stated that "[u]nder the private-search doctrine, the government does not conduct a Fourth Amendment search when there is a 'virtual certainty' that its search will disclose nothing more than what a private party's earlier search has revealed." (citing United States v. Jacobsen, 466 U.S. 109, 119, 104 S.Ct. 1652 (1984)). Thus, the issue is whether Bailey's search would disclose anything more than what Kik's search and the Cybertip showed. *See id*. Here, the court finds that Agent Bailey's conduct did not amount to a trespass by taking the files from NCMEC and then viewing these files since they had already been viewed and identified by Kik as containing apparent child pornography. As the government concludes, (Doc. 37 at 12), "it is clear that NCMEC contacted the government pursuant to their reporting requirement, and provided the government with the information provided by Kik. The government received the property from NCMEC

and reviewed it, after a private entity had already determined that it contained child pornography and voluntarily provided those images to NCMEC." (citation omitted).

Finally, the court finds no merit to Hart's argument that "the viewing of the files identified by K[ik] as apparent child pornography does not mean that the files contained child pornography" and that "Agent Bailey has special training to make [such] assessments." The Cybertip indicated that Kik viewed the entire contents of the uploaded files, that some of the files were shared in a messaging group on Kik by the user televiper and, that some of the files were sent from televiper to other users via private chat message. (Doc. 33-1). The Cybertip also contained a description of what Kik found in viewing the files, "apparent child pornography." Agent Bailey subsequently opened the same files and also determined that they contained child pornography. Moreover, there has been no allegation and no evidence that Agent Bailey exceeded the scope of his authority when he relied on the information Kik provided in the Cybertip after its private search. As the Supreme Court found in Jacobsen, 466 U.S. at 117, "the Fourth Amendment does not prohibit governmental use of the now-nonprivate information."[3]

[3]The government does not alternatively argue that even if there was a 4th Amendment violation in this case, the good faith exception should preclude exclusion of the evidence basically because when Agent Bailey reviewed the files contained with Kik's Cybertip and obtained the search warrant for Hart's home, he had no reason to believe that Kik had provided NCMEC with information procured in violation of Hart's 4th Amendment rights. The court notes that some courts have found the good faith exception applies in similar cases. *See* Tolbert, 326 F.Supp.3d

IV. CONCLUSION

For the aforementioned reasons, Defendant Hart's suppression motion, **(Doc. 32)**, is **DENIED IN ITS ENTIRETY**. An appropriate Order follows.

s/ Malachy E. Mannion
MALACHY E. MANNION
United States District Court

Dated: June 14, 2021
20-197-01

---

at 1121-1124 (holding that law enforcement "naturally assumed that the statutory authority granted to NCMEC was enough to justify opening the emails", and that "a reasonable law enforcement officer could conclude that by opening an email or attachment that NCMEC had already opened, he was merely repeating a search previously performed by a private party as permitted by the private search doctrine.") (citing United States v. Stratton, 229 F.Supp.3d 1230, 1233 (D. Kan. 2017); United States v. Keith, 980 F.Supp.2d 33 (D. Mass. 2013)).